

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
27 December 2002 (27.12.2002)

PCT

(10) International Publication Number  
**WO 02/103968 A1**

(51) International Patent Classification<sup>7</sup>: **H04L 12/58**,  
G06F 11/34

(21) International Application Number: PCT/NO02/00210

(22) International Filing Date: 14 June 2002 (14.06.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
20012994 15 June 2001 (15.06.2001) NO

(71) Applicant (for all designated States except US): **BEEP SCIENCE AS** [NO/NO]; Karenslyst Allé 16d, N-0214 Oslo (NO).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **NILSEN, Børge** [NO/NO]; Lørenveien 34, N-0585 Oslo (NO). **BREIVIK, Øyvind** [NO/NO]; Ullevålsveien 49, N-0171 Oslo (NO).

(74) Agent: **OSLO PATENTKONTOR AS**; P.O. Box 7007 M, N-0306 Oslo (NO).

(81) Designated States (*national*): AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

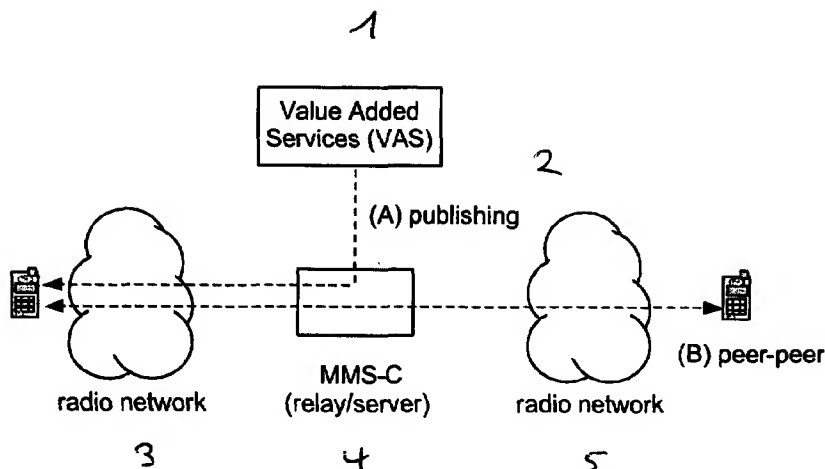
(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Declarations under Rule 4.17:**

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES.

[Continued on next page]

(54) Title: AN ARRANGEMENT AND A METHOD FOR CONTENT POLICY CONTROL IN A MOBILE MULTIMEDIA MESSAGING SYSTEM



(57) Abstract: A method and an arrangement for enforcement and control of copyright and/or policy of a data object being transferred in a communication network by generating an electronic fingerprint unique to the electronic element is disclosed. The fingerprint is compared with pre-generated electronic fingerprints stored in a database wherein each of said pre-generated fingerprints is linked to a certain policy and/or copyright concerning the fingerprint associated data object. If the electronic fingerprint matches one of the pre-generated electronic fingerprints, the policy and/or copyright restrictions linked thereto is/are enforced. The present invention is particularly useful in an MMS environment, and meets the requirements for content rights control in the MMS service network.



FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, *ARIPO patent* (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), *Eurasian patent* (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), *European patent* (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), *OAPI patent* (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— of inventorship (Rule 4.17(iv)) for US only

**Published:**

— with international search report

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

## **An arrangement and a method for Content Policy Control in a Mobile Multimedia Messaging System**

### Field of the invention

The present invention relates to an arrangement and a  
5 method for enforcement and control of copyright and/or po-  
lity of data objects being transferred in a communication  
network. In particular, this invention relates to enforce-  
ment and control of copyrights and policies of data objects  
in messaging environments where value added content can be  
10 published, e.g. in Multimedia Messaging Service (MMS) en-  
vironments.

### Background of the invention

Message services like SMS in GSM went through a fast growth  
just a few years after the worldwide launching of digital  
15 mobile communication network, and they are still growing in  
popularity. The recent exponential growth of e.g. value  
added Short-Messaging-Services (SMS) was triggered by the  
introduction of distribution and billing opportunities,  
provided by the mobile operators, to 3rd party value added  
20 service (VAS) and content providers. Some examples of VAS  
SMS are jokes (text format), stock quotes (text format),  
simple ringing tones (binary format), black-and-white logos  
(binary format).

However, the fact that the first generation message ser-  
25 vices are text based will probably threaten their existence  
in the near future, taking into account that multimedia  
services turns out to be customary.

Because of this, the WAP forum and 3GPP have standardized a  
new message service for the mobile environment called Mul-  
30 timedia Messaging Service (MMS) [1]. To the end-user, MMS  
is very similar to the Short Message Service (SMS): it pro-  
vides automatic immediate delivery for user created content  
from phone to phone.

However, the future of VAS MMS services has an even greater growth potential due to the advanced content capabilities of the MMS technology. Sophisticated multimedia content may be provided with VAS MMS services. Some examples of envis-  
5 aged value added MMS and content are "mobile greeting card portal" (such as sending pictures/animations, with or without sound from a portal to a mobile terminal), "famous cartoon messages" (such as animations, with or without colours/audio), "visual/audio quiz messages" (such as picture/audio messaging games), "talking head message" (such  
10 as rendering a personal text with a predefined animation). VAS MMS will be offered to the end users by operators and by independent 3rd party service and content providers (e.g. media houses, portals, broadcasting corporations)  
15 that utilise the wireless MMS infrastructure of the operators.

Multimedia content has an inherently greater value to the content owners than plain text content (e.g. SMS). When publishing such content, it is important to the content  
20 providers or content owners that the content rights (copyrights and policies) are enforced and that their revenue streams are secured. If not, the content providers will naturally not be interested in producing content for use in MMS. The publishing process thus needs to support copyright  
25 control and ensure that defined content policies are being obeyed.

To increase MMS traffic, the mobile operator has to provide a solution to support these requirements allowing content owners to publish their content for value added MMS.

30 Current attempts on content control are oriented towards the Internet model. The models normally require updates both to the content production process and to the client software rendering the resulting content.

Two strategies are established for copyright control of  
35 Internet content. These are:

Digital watermark [2] that is a process where a pattern is added to the content. This pattern shall ideally be invisible for the end-user, whereas the copyright control can filter and recognise this pattern.

5 The clearinghouse [3] model is a model where the content is packaged in a container. When reading the content with a client that can interpret the specially packaged container, the container will authorize access to the content with a remote clearinghouse.

10 One strategy is established for policy control of Internet content. This is:

Platform for Internet Content Selection (PICS) [4] and Digital Signature (DSiG) [5] is a standard solution for defining and controlling meta-data for web content. This solution defines a language and a set of processing rules for  
15 controlling access to content. This allows e.g. parents to control what content their kids can access.

The problems with the prior art are specified in the following for each of the alternatives described above.

20 For the Digital Watermarking model, the problems are:

1. The solution cannot be used for all types of content
2. The solution requires updates to the content production process
3. The copyright control will be broken if the watermark  
25 is removed

For the clearinghouse model, the problems are:

1. The solution requires updates to the content production process

2. The solution requires special client software
3. Control process is coupled to access of content rather than delivery of it
  - a. This gives reduced security
  - 5       b. Control and payment is always coupled with receiver (limiting business model)
4. The establishment of new business roles (the clearing-house) is normally required
5. Integration with existing systems in the mobile operator domain is difficult  
10
6. The solution normally builds on digital certificates and Public Key Infrastructure. This may slow down/complicate rollout of system (requires established policies).

15 For the PICS/ DSiG solution, the problems are:

1. Requirement of special client software (PICS enabled browsers)
2. Rating of content needs to be carried out (long process)
- 20 3. Solution can be bypassed/ turned off as it is controlled by the end-user
4. No complete solution for rights control for value added content (in a mobile environment) is provided

#### Summary of the invention

- 25 It is an object of the present invention to provide an arrangement and a method that eliminates the drawbacks de-

scribed above. The features defined in the claims enclosed characterize this method.

More specifically, the present invention provides a method and an arrangement for enforcement and control of copyright  
5 and/or policy of a data object being transferred in a communication network by generating an electronic fingerprint unique to the electronic element. The fingerprint is compared with pre-generated electronic fingerprints stored in a database wherein each of said pre-generated fingerprints  
10 is linked to a certain policy and/or copyright concerning the fingerprint associated data object. If the electronic fingerprint matches one of the pre-generated electronic fingerprints, the policy and/or copyright restrictions linked thereto is/are enforced.

15 The present invention is particularly useful in an MMS environment, and meets the requirements for content rights control in the MMS service network. A preferred embodiment is a network centric model that is based on a fire-wall/gatekeeper model, where all messages are relayed  
20 through a control node where a filtering process is applied. This filtering process fingerprints all transferred content and applies content policy control to the content of these messages. The solution works with all existing content and does not require updates to the client software  
25 (terminals).

The process for content policy control consists of two phases. When content is being published, a fingerprint is generated and stored in a lookup table with a reference to the policy meta-data for this content. When later content  
30 is transferred between clients, the same fingerprint is generated and used to look up the policy reference, thus enabling the policy to be enforced.

The preferred embodiment proposes a Digital Rights Unit (DRU) consisting of 3 main components:

- A Policy Management Client (PMC), that is used for defining content policies
- A Content Control Engine (CCE), that maps policies to transferred content, and
- 5     - A Policy Enforcement Engine (PEE), that enforces the content policies

#### Brief description of the drawings

In order to make the invention more readily understandable, the discussion that follows will refer to the accompanying  
10 drawings.

Figure 1 illustrates MMS architecture and the components involved in message transfer between mobile handsets (peer-peer) and from a network server to a mobile handset (publishing).

15     Figure 2 illustrates the components involved in the MMS publishing process and how these components interact according to an example embodiment of the present invention.

Figure 3 illustrates the components involved in the MMS message transfer process for peer-peer communication between two mobile handsets according to an example embodiment of the present invention.  
20

#### Detailed description of preferred embodiments

The present invention will in the following be described in an MMS environment referring to the above-mentioned figures. However, this does not represent any limitations to  
25 the invention. The present invention may be utilized in other similar applications, environments and contexts with other variations and substitutions without departing from the scope of the invention as defined by the attached independent claims.  
30



The MMS message delivery process for value added content is depicted in figure 1. As illustrated, the message transfer may either be initiated from the network (i.e. published) or it may be initiated from a peer terminal (user-agent).  
5 For value added content that is subject to policy control, the first delivery will always be initiated from the network (i.e. published). The published content may then be distributed (forwarded) in a peer-peer fashion. The invention builds on this nature for the distribution of value  
10 added content.

The present invention meets the requirements for content rights control in the MMS service network. A preferred embodiment of the present invention is a network centric model that is based on a firewall/ gatekeeper model, where  
15 all messages are relayed through a control node where a filtering process is applied. This filtering process fingerprints all transferred content and applies content policy control to the contents of these messages. The solution works with all existing content and does not require up-  
20 dates to the client software (terminals).

Examples of content and content elements that may comprise value added content/service data are audio files, pictures, animations, video, and text, and any combination of these.

The process for content policy control consists of two  
25 phases. When content is being published, a fingerprint is generated and stored in a lookup table with a reference to the policy meta-data for this content. When later content is transferred between clients, the same fingerprint is generated and used to look up the policy reference, thus  
30 enabling the policy to be enforced.

The preferred embodiment proposes a Digital Rights Unit (DRU) consisting of 3 main components: a Policy Management Client (PMC), a Content Control Engine (CCE), and a Policy Enforcement Engine (PEE).

### **The Policy Management Client**

The PMC defines and activates the content policies of the controlled content. It consists of a client interface where  
5 policies may be created, updated and deleted, and a control function that initiates content control when content is being published.

### **The Content Control Engine**

The CCE filters the messages being transferred. It may be  
10 deployed as a standalone relay or it may be integrated with other message relay functions. When a message is received, the CCE will analyse the components of the message and apply policy control to the respective message components.

MMS messages are multipart-MIME [6] encoded with message  
15 blocks for each message element. The message elements are separated with MIME headers that define the content (e.g. the type and size). The CCE will typically analyse these header fields and use them to invoke content specific control functions.

20 For each message component, the CCE will analyse the content-type and apply a content specific control function (i.e. switching-control function based on content-type). The invoked control function will then generate a fingerprint for the given content and check it against a local  
25 fingerprint database. If a hit is found, the CCE will return a URL [7] that identifies the policy to be applied for that content.

For a message consisting of multiple content-elements, several control functions will be invoked, possible resulting  
30 in several policies being identified and enforced.

### **The Policy Enforcement Engine**

The PEE enforces the policies that the CCE identifies. When

being invoked with a new policy statement, it effectuates the policy and tells the client (the CCE or the PMC) if the content is allowed. In effectuating the policy, the PEE controls access rights to the content and generates the content charge information.

In order to describe the process of content distribution and rights control, a typical usage scenario will now be described. The typical scenario consists of three steps, being the policy definition process, the publishing process and the transfer control process.

### **The Policy Definition Process**

In the policy definition process, the content owner makes a value added content available, i.e. it is stored in a server/database connected to the communication network. At the same time, the associated content policy (e.g. meta-data) in the same or a different server/database.

### **The Publishing Process**

The publishing process applies to content being delivered from a network server to a client terminal and its user-agent. The traffic flow is depicted in figure 1 and labelled with (A) publishing.

The Policy Management Client (PMC) carries out control of content being published (i.e. content being sent from a network server to an end-user). The PMC will check if the published content has a defined policy and make sure that the policy is enforced and activated.

The PMC may use different techniques to identify the policy of a content element. The content elements and policies are all identified by URLs (Uniform Resource Locator) [7].

- a. A separate database may be used to map content URL to policy URL. Such a database will be written/updated when new content or policies are published.

b. Wrapper files containing both the reference to the content and the policy may be used. The PMC will separate the content and the policy from the wrapper file.

5 c. A shadow policy directory (URL) may be used to map the policy to the content. In this case, all content URLs have a shadow policy URL where there is a fixed relation between the two URLs (e.g. /image/cool.gif -> /image/cool\_gif.policy).

10 When the PMC identifies a content element with a policy, it will request the Policy Enforcement Engine (PEE) to process the policy. In doing so, the PMC provides a reference to the policy and the identity of the message receiver. The PEE will then process this policy and return an ok status code if the content is allowed in this context. Content  
15 that is not allowed in the given context will be removed or replaced with a screening message (e.g. "Content requested not allowed") by the PMC before the message is delivered.

20 When the Policy Enforcement Engine (PEE) is invoked to enforce a policy, it will do the following steps (or any combinations thereof) to enforce the policy:

a. Check if the receiver is allowed to receive the content element from the sender. The check is performed by retrieving user information (e.g. address, age, prepaid account level) either from an independent database containing such information or from the data-  
25 base of the mobile operator and checking the user information with the content policy (e.g. age group allowed, price policy, number series allowed).

30 b. Generate charging information to charge the sender for use of the content element.

When access to content is granted, the PMC activates the policy control by generating a fingerprint for this content and adding that fingerprint and its associated policy ID to the fingerprint database.

### The Transfer Control Process

The content transfer control process applies to content being transferred between two terminals and their user-agents. The traffic flow is depicted in figure 1 and labelled with (B) peer-peer.

The Content Control Engine (CCE) carries out control of transferred content. It may either be deployed as a stand-alone relay or it may be integrated with the MMS-C relay functions [1]. The task of the CCE is to filter transferred messages, identify the message elements and for each message element generate a fingerprint and check if this fingerprint has a defined policy.

Examples of content and content elements that may comprise value added content/service data in a message and that is to be filtered, are audio files, pictures, animations, video, and text, and any combination of these.

When the CCE identifies a content element with a policy, it will request the Policy Enforcement Engine (PEE) to process the policy. In doing so, the CCE provides a reference to the policy and the identity of the message sender and receiver respectively. The identities of the message sender and receiver are retrieved by the CCE from the message elements. The PEE will then process this policy and return an ok status code if the content is allowed in this context. Content that is not allowed in the given context will be removed or replaced with a screening message by the CCE before the message is delivered.

When the Policy Enforcement Engine (PEE) is invoked to enforce a policy, it will undergo the following steps (or any combination thereof) to enforce the policy:

- a. Check if the sender is allowed to send the content element to receiver

b. Check if the receiver is allowed to receive the content element from the sender.

c. Generate charge information to charge the sender for use of the content element

5 The check (a, b) is performed by retrieving user information (e.g. address, age, prepaid account level) either from an independent database containing such information or from the database of the mobile operator and checking the user information with the content policy (e.g. age group allowed, price policy, forwarding allowed/not allowed, number series allowed).

In the following, some supplemental information regarding parts of the process and architecture discussed above is disclosed.

#### 15 **Identifying Message Elements**

During the process of analyzing message content, the PMC and CCE need to identify the message elements. This is done based on the MIME message encoding used for MMS messages. This message encoding separates each message element as a separate block in the message with separate message headers, such as content-type.

Some examples of content-types (with associated formats) are GIF[8], JPEG[9], MP3[10], MPEG4[11], AMR [12].

25 The PMC and CCE rely on the MIME message encoding and will switch control routines based on the content-type presented. This allows content-specific specialization of routines used for generation of fingerprints and database lookup. This also allows the control routines to be distributed, e.g. using one server for handling of image policies and another server for audio policies.

#### **Generation of Fingerprints**

Routines for generating fingerprints may be specialized per content-type. This allows new advanced fingerprint routines to be added on the fly as soon as new algorithms become available. Adding a new fingerprint routine consists of  
5 adding a new code entity (e.g. java class) and configuring the binding between content-type and class name.

Examples of algorithms are: MD4[13] and MD5[14].

### **The Fingerprint Database**

The fingerprint database is a table that matches fingerprints with policy ID. The table is close to routing/  
10 relaying of messages and needs to provide fast lookup.

The fingerprint database needs to have a limited size and defined policy for how to handle table overflow (cache aging policies) and leakage (cache leakage causing missing  
15 entries). Preferably, a policy that accepts a fraction of overflow and leakage and builds that into the publishing model (all commerce solutions have a fraction of failed transactions, i.e. leakage, and this invention uses that fact to make a more efficient solution) is used.

20 To reduce the amount of overflow and leakage, several solutions may be used. The simplest alternative is to increase the size of the table. Other alternatives are to use content specific tables or have separate table areas per user. A preferred embodiment of the invention allows the security  
25 to be balanced against performance and cost at setup and configuration time.

### **The Policy Database**

The fingerprint database is a database of XML [15] formatted meta-data elements. Each meta-data element defines the  
30 policy for a given content element. The policy defines rules for accessing the content and content charges.

The policy database can easily be integrated with existing content databases and extend the functionality of these. This also supports integration with the provisioning systems of the operators and portals.

5 One advantage of the present invention is that it provides a secure solution for the mobile operator to handle enforcement and control of copyrights and policies for published content.

10 In addition, the invention provides a solution that extends the mobile operator's business model, supporting not only charging of value added content for the content owners, but also enforcement and control of the content owners' copyrights and content policies with flexible business models (e.g. sender or receiver may be charged).

15 The present invention also integrates with the mobile operator's domain and infrastructure and cannot be by-passed in the message transfer process (i.e. good security, and forwarding of messages can be handled properly with enforcement and control and with the desired business models).

20 The invention may be deployed by the mobile operator as a stand-alone component within the mobile infrastructure or it may be deployed as an integrated component with other components (e.g., MMS-C) for optimization purposes. It does not rely on software updates to mobile terminals and their user-agents, i.e. terminal vendor independence, paramount to commercial applicability.

A further advantage of the present invention is that it may be used for all content types. It does not require updates to the content production process.

30 Further, the invention does not add content overhead (such as meta-data, watermark data) in the messages being transported within the network and thus does not require extra message transport capacity.



The invention provides a fingerprinting solution that is inherently fast/efficient (small sized fingerprints solution with fast algorithms are available, e.g. MD4), computational unique for content, may be optimized with different algorithms for specific content types, and may easily  
s be upgraded (easy plug-in scheme) with new algorithms for specific content types as new and better/faster algorithms become available.

### References

- [1] **MMS** 3GPP TS 23.140 v4.2.0 (2001-03), 3rd Generation Partnership Project; Technical Specification Group Terminals; Multimedia Messaging Service (MMS); Functional description; Stage 2 (Release 4)  
5
- [2] **Digital Watermark** "Digital Watermarks Copyright Protection for Online Artists", PC Magazine, February 18. 1997
- [3] **Clearinghouse** "Digital Rights for all media types", Internetcontent.net, 2/20/2001
- 10 [4] **PICS** Rating Services and Rating Systems (and Their Machine Readable Descriptions), REC-PICS-services-961031, version 1.1, World Wide Web Consortium (W3C), Recommendation 31-October-1996
- [5] **DSig** PICS Signed Labels (DSig) 1.0 Specification, REC-  
15 DSig-label-19980527, World Wide Web Consortium (W3C), Recommendation 27-May-1998
- [6] **MIME** Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, Internet Engineering Task Force (IETF), Request For Comment (RFC) 2045, November  
20 1996
- [7] **URL/URI**, Uniform Resource Identifiers (URI): Generic Syntax, Internet Engineering Task Force (IETF), Request For Comment (RFC) 2396, August 1998
- [8] **GIF**, Graphics Interchange Format (Version 89a),  
25 Compuserve Inc., Colombus, Ohio, 1990
- [9] **JPEG**, ITU-T Rec. T.81/ISO/IEC 10918-1: 1992, „Information Technology - Digital Compression and Coding of Continuous-Tone Still Images - Requirements and Guidelines".

- [10] **MP3** MPEG1-Audio ISO/IEC 11172-3, MPEG2-Audio ISO/IEC 11172-3
- [11] **MPEG4**, ISO/IEC 14496-1(1999): Information Technology - GenericCoding of Audio-Visual Objects AND 3GPP TR 26.911:  
5 "Codec(s) for Circuite Switched Multimedia Telephony Service; Terminal Implementor's Guide"
- [12] **AMR** 3GPP TS 26.090: "AMR Speech Codec Speech Transcoding Functions"
- [13] **MD4** The MD4 Message-Digest Algorithm, Internet  
10 Engineering Task Force (IETF), Request For Comment (RFC) 1320, April 1992
- [14] **MD5** The MD5 Message-Digest Algorithm, Internet Engineering Task Force (IETF), Request For Comment (RFC) 1321, April 1992
- 15 [15] **XML** Extensible Markup Language (XML) 1.0 (Second Edition), World Wide Web Consortium (W3C), Recommendation 6 October 2000

**P a t e n t   c l a i m s**

1.    An arrangement for enforcement and control of  
copyright and policy of a data object being transferred in  
a communication network,  
5    c h a r a c t e r i z e d   i n  
  
        a first means adapted to generate an electronic  
fingerprint unique to said data object,  
  
        a fingerprint database comprising pre-generated  
electronic fingerprints of data objects, each of which  
10    are linked to a certain policy and/or copyright  
concerning current fingerprint associated data object,  
  
        a second means adapted to compare said fingerprint  
with said pre-generated fingerprints,  
  
        a third means adapted to enforce the policy and/or  
15    copyright restrictions linked to said one of the pre-  
generated electronic fingerprints on said data object  
if said electronic fingerprint matches one of the pre-  
generated electronic fingerprints.
2.    Arrangement according to claim 1,  
20    c h a r a c t e r i z e d   i n  
  
        a fourth means adapted to define, activate, create,  
update and/or delete said policy and/or copyright  
through an interface therein.
3.    Arrangement according to claim 1 or 2,  
25    c h a r a c t e r i z e d   i n    that said data object is,  
or is an element of, a Multimedia Message Service (MMS)  
message, and that said database and/or said first, second,  
third and/or fourth means are integrated in, or connected  
to, an MMS architecture.
- 30    4.    Arrangement according to claim 3,  
c h a r a c t e r i z e d   i n

a fifth means adapted to identify and separate said element in said MMS message.

5. Arrangement according to any of the preceding claims, characterized in that each of the pre-generated electronic fingerprints is generated by said first means and stored in said database as its associated data object is transmitted to a user requesting that data object.

6. Arrangement according to any of the preceding claims, characterized in that said policy comprises rules for executing said data object and/or charging a user sending, receiving or requesting said data object.

7. Arrangement according to claim 6, characterized in that said rules include filtering away, replacing and/or changing said data object when a certain receiver or sender of said data object is identified.

8. Arrangement according to claim 6 or 7, characterized in that said policy is stored in a separate policy database, and that information concerning said charging is written into a separate charging database.

9. Arrangement according to any of the preceding claims, characterized in that the pre-generated electronic fingerprints are stored in a look up table and that each of which are linked to a certain policy and/or copyright concerning current fingerprint associated data object by a URL.

10. Arrangement according to any of the preceding claims, characterized in that the said database is a database of XML formatted meta-data elements.

11. Arrangement according to any of the preceding claims,  
c h a r a c t e r i z e d i n that said communication  
network is a GSM, GPRS, or UMTS network.

12. Arrangement according to any of the preceding claims,  
5 c h a r a c t e r i z e d i n that said data object  
comprises value added content issued by a content provider.

13. Arrangement according to any of the preceding claims,  
c h a r a c t e r i z e d i n that said data object is  
transferred through said communication network on a peer-  
10 to-peer basis, i.e. from a first user terminal to a second  
user terminal.

14. Arrangement according to any of the preceding claims,  
c h a r a c t e r i z e d i n that said data object is  
an audio file, a picture, an animation, a video, a text  
15 string or any combination of these.

15. Arrangement according to any of the preceding claims,  
c h a r a c t e r i z e d i n that said first means  
includes routines for generating fingerprints specialized  
per data object type.

20 16. Arrangement according to claim 15,  
c h a r a c t e r i z e d i n that said first means is  
adapted to incorporate any new routine for generating  
fingerprints in addition to the already included.

17. A method for enforcement and control of copyright  
25 and/or policy of a data object being transferred in a  
communication network,  
c h a r a c t e r i z e d i n the following steps:

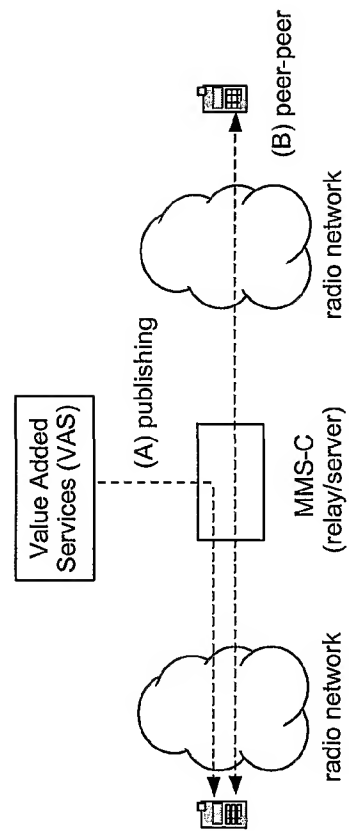
a) Generating an electronic fingerprint unique to  
said data object,

30 b) Comparing the electronic fingerprint with pre-  
generated electronic fingerprints stored in a  
database wherein each of said pre-generated

fingerprints are linked to a certain policy and/or copyright concerning current fingerprint associated data object,

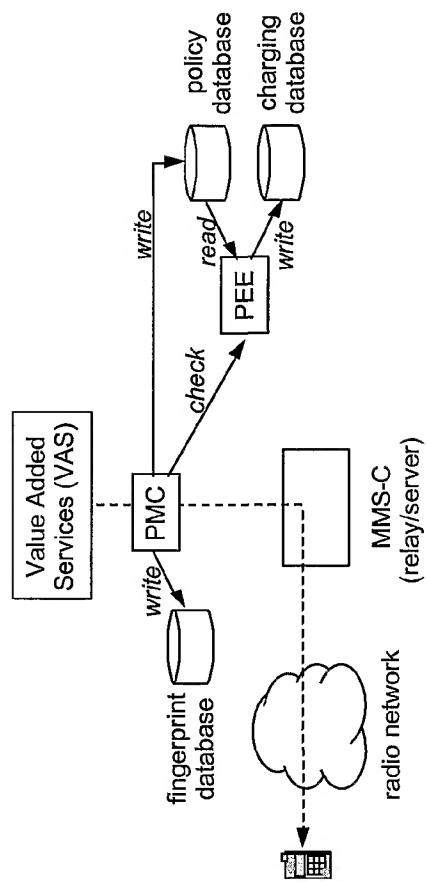
- 5 c) If said electronic fingerprint matches one of the pre-generated electronic fingerprints in step b), enforcing the policy and/or copyright restrictions linked to said one of the pre-generated electronic fingerprints on said data object.

1/3

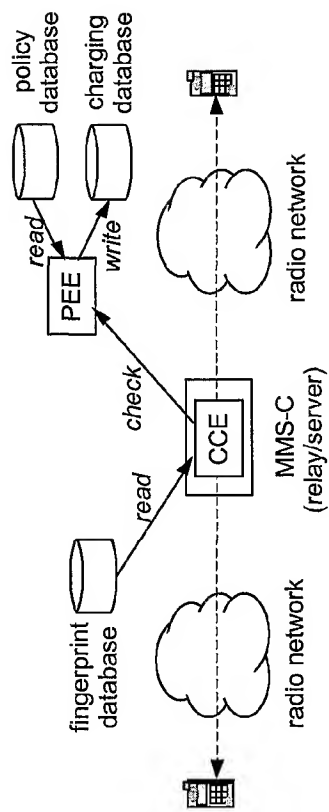
**Fig. 1**



2/3

**Fig. 2**

3/3

**Fig. 3**

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/NO 02/00210

## A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/58, G06F 11/34

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 0115405 A2 (ADWISE LTD), 1 March 2001 (01.03.01), page 5, line 29 - page 6, line 9; page 8, line 4 - line 14 --	1-17
X	WO 0072119 A2 (RABIN, M. ET AL.), 30 November 2000 (30.11.00), claims 1-137 --	1-17
X	US 6144934 A (STOCKWELL, E.B. ET AL.), 7 November 2000 (07.11.00), claim 19 --	1-17
A	US 6141753 A (ZHAO, J. ET AL.), 31 October 2000 (31.10.00), see the whole document --	1-17

☒ Further documents are listed in the continuation of Box C.
 ☒ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;" document member of the same patent family

Date of the actual completion of the international search

27 August 2002

Date of mailing of the international search report

12-09-2002

Name and mailing address of the ISA/

Swedish Patent Office

Box 5055, S-102 42 STOCKHOLM

Facsimile No. +46 8 666 02 86

Authorized officer

Kristoffer Ogebjer/LR

Telephone No. +46 8 782 25 00

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/NO 02/00210

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	HEINTZE, N.: Scalable Document Fingerprinting (1996) 1996 USENIX Workshop on Electronic Commerce See the whole document  --	1-17
A	RIVEST, R.: The MD5 Message-Digest Algorithm. MIT Laboratory for Computer Science and RSA Data Security, Inc. April 1992 Network Working Group, Request for comments: 1321. See whole document  --	1-17
A	US 6173401 B1 (DEINDL, M. ET AL.), 9 January 2001 (09.01.01), abstract  -- -----	1-17

# INTERNATIONAL SEARCH REPORT

Information on patent family members

06/07/02

International application No.

PCT/NO 02/00210

Patent document cited in search report			Publication date	Patent family member(s)		Publication date
WO	0115405	A2	01/03/01	AU	6586700 A	19/03/01
WO	0072119	A2	30/11/00	AU	4813700 A	12/12/00
				EP	1180252 A	20/02/02
US	6144934	A	07/11/00	DE	19741238 A,C	02/04/98
				GB	2317793 A,B	01/04/98
				GB	9719820 D	00/00/00
US	6141753	A	31/10/00	CA	2319340 A	19/08/99
				EP	1055321 A	29/11/00
				JP	2002503838 T	05/02/02
				WO	9941900 A	19/08/99
US	6173401	B1	09/01/01	DE	19716015 A	29/10/98
				GB	2324894 A,B	04/11/98
				GB	9804703 D	00/00/00
				JP	10301854 A	13/11/98